FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1639656-000

Total Deleted Page(s) = 253
Page 9 ~ b4;
Page 10 ~ b4;
Page 11 ~ b4;
Page 12 ~ b4;
Page 13 ~ b4;
Page 14 ~ b4;
Page 15 ~ b4;
Page 16 ~ b4;
Page 17 ~ b4;
Page 25 ~ b3; b6; b7C; b7E; OTHER;
Page 26 ~ b3;
Page 27 ~ b3; b7E;
Page 28 ~ b3; b7E;
Page 29 ~ b3;
Page 30 ~ b3; b7E;
Page 31 ~ b3;
Page 32 ~ b3;
Page 33 ~ b3;
Page 34 ~ b3; b7E;
Page 35 ~ b3; b7E;
Page 36 ~ b3;
Page 37 ~ b3; b7E;
Page 38 ~ b3; b7E;
Page 39 ~ b3; b7E;
Page 40 ~ b3; b7E;
Page 41 ~ b3; b7E;
Page 42 ~ b3; b7E;
Page 43 ~ b3; b7E;
Page 44 ~ b3; b7E;
Page 45 ~ b3; b7E;
Page 46 ~ b3; b7E;
Page 47 ~ b3; b7E;
Page 48 ~ b3; b7E;
Page 49 ~ b3; b7E;
Page 50 ~ b3; b6; b7C; OTHER;
Page 51 ~ b3; b7E;
Page 52 ~ b3; b6; b7C;
Page 53 ~ b3; b7E;
Page 54 ~ b3; b6; b7C; b7E;
Page 55 ~ b3; b7E;
Page 56 ~ b3; b6; b7C; b7E;
Page 57 ~ b3; b6; b7C;
Page 58 ~ b3;
Page 59 ~ b3; b6; b7C; b7E;
Page 60 ~ b3; b6; b7C; b7E;
Page 61 ~ b3; b7E;
Page 62 ~ b3; b7E;
Page 63 ~ b3; b7E;
Page 64 ~ b3; b7E;
Page 65 ~ b3; b7E;
Page 66 ~ b3; b7E;
Page 67 ~ b3; b7E;
Page 71 ~ b4;
Page 73 ~ b4;
Page 74 ~ b4;
Page 75 ~ b4;
Page 76 ~ b4;
Page 77 ~ b4;
Page 78 ~ b4;
Page 79 ~ b4;
Page 81 ~ b3; b6; b7C; OTHER;
Page 82 ~ b3; b6; b7C;
Page 83 ~ b3; b6; b7C;
Page 86 ~ b3;
Page 87 ~ b6; b7C;
Page 88 ~ b6; b7C;
Page 89 ~ b6; b7C;

Page 90 ~ b3; b6; b7C; b7E;
Page 91 ~ b3; b7E;
Page 92 ~ b3; b7E;
Page 93 ~ b3; b7E;
Page 94 ~ b3; b7E;
Page 95 ~ b3; b7E;
Page 96 ~ b3; b7E;
Page 97 ~ b6; b7C;
Page 98 ~ b6; b7C;
Page 99 ~ b6; b7C;
Page 100 ~ b6; b7C;
Page 101 ~ b6; b7C;
Page 102 ~ b6; b7C;
Page 103 ~ b6; b7C;
Page 104 ~ b6; b7C;
Page 105 ~ b6; b7C;
Page 106 ~ b6; b7C;
Page 107 ~ b6; b7C;
Page 108 ~ b6; b7C;
Page 109 ~ b6; b7C;
Page 110 ~ b6; b7C;
Page 111 ~ b6; b7C;
Page 112 ~ b6; b7C;
Page 113 ~ b6; b7C;
Page 114 ~ b6; b7C;
Page 115 ~ b6; b7C;
Page 116 ~ b6; b7C;
Page 117 ~ b6; b7C;
Page 118 ~ b6; b7C;
Page 119 ~ b6; b7C;
Page 120 ~ b6; b7C;
Page 121 ~ b6; b7C;
Page 122 ~ b6; b7C;
Page 123 ~ b6; b7C;
Page 124 ~ b6; b7C;
Page 125 ~ b6; b7C;
Page 126 ~ b6; b7C;
Page 127 ~ b6; b7C;
Page 128 ~ b6; b7C;
Page 129 ~ b6; b7C;
Page 131 ~ Referral/Consult;
Page 132 ~ Referral/Consult;
Page 133 ~ Referral/Consult;
Page 140 ~ Referral/Consult;
Page 141 ~ Referral/Direct;
Page 142 ~ Referral/Direct;
Page 143 ~ Referral/Direct;
Page 148 ~ Referral/Direct;
Page 149 ~ Referral/Direct;
Page 150 ~ Referral/Direct;
Page 151 ~ Referral/Direct;
Page 152 ~ Referral/Direct;
Page 153 ~ Referral/Direct;
Page 154 ~ Referral/Direct;
Page 155 ~ b4;
Page 156 ~ b4;
Page 157 ~ b4;
Page 158 ~ b4;
Page 159 ~ b4;
Page 160 ~ b4;
Page 161 ~ b4;
Page 162 ~ b4;
Page 163 ~ b4;
Page 164 ~ Referral/Consult;
Page 178 ~ Referral/Direct;
Page 179 ~ Referral/Direct;
Page 180 ~ Referral/Direct;
Page 181 ~ Referral/Direct;
Page 182 ~ Referral/Direct;
Page 183 ~ Referral/Direct;
Page 190 ~ b6; b7C;
Page 191 ~ b6; b7C;
Page 192 ~ b6; b7C;

Page 193 ~ b6; b7C;
Page 200 ~ b6; b7C; b7E;
Page 201 ~ b6; b7C; b7E;
Page 208 ~ Referral/Direct;
Page 209 ~ Referral/Direct;
Page 210 ~ Referral/Direct;
Page 211 ~ Referral/Direct;
Page 212 ~ Referral/Direct;
Page 213 ~ Referral/Direct;
Page 214 ~ Referral/Direct;
Page 215 ~ Referral/Direct;
Page 216 ~ Referral/Direct;
Page 217 ~ Referral/Direct;
Page 218 ~ Referral/Direct;
Page 219 ~ Referral/Direct;
Page 220 ~ Referral/Direct;
Page 221 ~ Referral/Direct;
Page 222 ~ Referral/Direct;
Page 223 ~ Referral/Direct;
Page 224 ~ Referral/Direct;
Page 225 ~ Referral/Direct;
Page 226 ~ Referral/Direct;
Page 227 ~ Referral/Direct;
Page 228 ~ Referral/Direct;
Page 229 ~ Referral/Direct;
Page 230 ~ Referral/Direct;
Page 231 ~ Referral/Direct;
Page 232 ~ Referral/Direct;
Page 233 ~ Referral/Direct;
Page 234 ~ Referral/Direct;
Page 235 ~ Referral/Direct;
Page 236 ~ Referral/Direct;
Page 237 ~ Referral/Direct;
Page 238 ~ Referral/Direct;
Page 239 ~ Referral/Direct;
Page 240 ~ Referral/Direct;
Page 241 ~ Referral/Direct;
Page 242 ~ Referral/Direct;
Page 243 ~ Referral/Direct;
Page 244 ~ Referral/Direct;
Page 245 ~ Referral/Direct;
Page 246 ~ Referral/Direct;
Page 247 ~ Referral/Direct;
Page 248 ~ Referral/Direct;
Page 249 ~ Referral/Direct;
Page 250 ~ Referral/Direct;
Page 251 ~ Referral/Direct;
Page 252 ~ Referral/Direct;
Page 253 ~ Referral/Direct;
Page 254 ~ Referral/Direct;
Page 255 ~ Referral/Direct;
Page 256 ~ Referral/Direct;
Page 257 ~ Referral/Direct;
Page 258 ~ Referral/Direct;
Page 259 ~ Referral/Direct;
Page 260 ~ Referral/Direct;
Page 261 ~ Referral/Direct;
Page 262 ~ Referral/Direct;
Page 263 ~ Referral/Direct;
Page 264 ~ Referral/Direct;
Page 265 ~ Referral/Consult;
Page 266 ~ Referral/Consult;
Page 267 ~ Referral/Consult;
Page 268 ~ Referral/Consult;
Page 269 ~ Referral/Consult;
Page 270 ~ Referral/Consult;
Page 271 ~ Referral/Consult;
Page 272 ~ Referral/Consult;
Page 273 ~ Referral/Direct;
Page 274 ~ Referral/Direct;
Page 275 ~ Referral/Direct;
Page 276 ~ Referral/Direct;
Page 277 ~ Referral/Direct;

Page 278 ~ Referral/Direct;
Page 279 ~ Referral/Direct;
Page 280 ~ Referral/Direct;
Page 281 ~ Referral/Direct;
Page 286 ~ Referral/Direct;
Page 287 ~ Referral/Direct;
Page 288 ~ Referral/Direct;
Page 289 ~ Referral/Direct;
Page 290 ~ Referral/Direct;
Page 291 ~ Referral/Direct;
Page 292 ~ Referral/Direct;
Page 293 ~ Referral/Direct;
Page 294 ~ Referral/Direct;
Page 295 ~ Referral/Direct;
Page 296 ~ Referral/Direct;
Page 297 ~ Referral/Direct;
Page 298 ~ Referral/Direct;
Page 299 ~ Referral/Direct;
Page 300 ~ Referral/Direct;
Page 301 ~ Referral/Direct;
Page 302 ~ Referral/Direct;
Page 303 ~ Referral/Direct;
Page 304 ~ Referral/Direct;
Page 305 ~ Referral/Direct;
Page 306 ~ Referral/Direct;
Page 307 ~ Referral/Direct;
Page 308 ~ Referral/Direct;
Page 309 ~ Referral/Direct;
Page 310 ~ Referral/Direct;
Page 311 ~ Referral/Direct;
Page 312 ~ Referral/Direct;
Page 313 ~ Referral/Direct;
Page 314 ~ Referral/Direct;
Page 315 ~ Referral/Direct;
Page 316 ~ Referral/Direct;
Page 317 ~ Referral/Direct;
Page 318 ~ Referral/Direct;
Page 319 ~ Referral/Direct;
Page 320 ~ Referral/Direct;
Page 321 ~ Referral/Direct;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

DECLASSIFIED BY [redacted]
ON 09-21-2012

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/04/1998

To: NSD/CID **Attn:** SSA [redacted]
OSIIP/CITAC/Rm 11887

From: Sacramento
WCC, Squad 5
Contact: SA [redacted]

.b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted] :mah

Case ID #: (U) ~~(S)~~ 288-HQ-1242560 167 (Pending)
(U) ~~(S)~~ [redacted] (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO;HQ

Synopsis: (U) ~~(S)~~ Information possibly pertaining to intrusions into DOD Domain Name Servers using the "statd" exploit on Solarus 2.4 operating systems.

(U) ~~(S)~~ ~~**Classified By: 10877, 4/sc**~~
~~**Reason : 1.5(c)**~~
~~**Declassify On: 03/04/2008**~~

Reference: (U) ~~(S)~~ HQ EC's dated 2/9/98, and 2/12/98.

Enclosures: (U) ~~(S)~~ Enclosed for FBIHQ/CITAC are the following:

1) 22 pages of logs provided by University of California-Davis.

2) 3 logs provided by the University of Colorado-Boulder.

(encloses sent to CA)

Details: (U) ~~(S)~~ On 2/2/98, [redacted] Computer Security Analyst, Information Resources, Division of Information Technology, University of California, 1 Shields Avenue, Davis, California, 95616, telephone [redacted] advised all 17,000 computers in the University of California-Davis (UCD) network have been attacked using a "statd" probe between 1/25/98 and 1/28/98. Page 6 of enclosure 1, UCD Incident Response Team (UCDIRT) notice #63, identified the initial probes as originating from netgate.saes.com. The initial attack lasted almost twenty-four hours. Three UCD hosts (ging.ucd.edu,

b6
b7C

~~SECRET~~

UPLOADED

junior.itd.ucdavis.edu, and guardian.ucdavis.edu) had TCP connections to other services during the attack. The Sun remote procedure connections from saes.com were the only ones logged in for that week. Saes.com was registered to St. Andrews School, Bethesda, Maryland. [redacted] was identified as the technical contact.

(U) (S) In the opinion of [redacted] UCDIRT leader, this attack was probably used to generate a list of hosts running "statd." The "statd" systems were then hit from computers located at Harvard University and Columbia University. Pages 7 through 10 of enclosure 1, identify the two computers at Harvard and Columbia as scotia.harvard.edu, and bone.tc.columbia.edu. Three hosts were intruded. The compromised computers were running Solaris 2.4.

(U) (S) [redacted] was the administrator for one of the compromised hosts in the Geology Department. After replacing Solaris 2.4 with Solaris 2.5.1, [redacted] examined logs from January 17, and 18, 1998. [redacted] discovered another "statd" attack. On January 18, 1998, the intruder gained root access. The origin of the attack appeared to be [redacted] Pages 4 and 5 of enclosure 1 represent examples of the "statd" attacks which occurred on January 17, and 18.

b6
b7C

(U) (S) [redacted] Associate Professor, Department of Computer Science, reviewed logs and discovered "imapd" probes during January 18, 1998, from [redacted] Page 3 of enclosure 1 is [redacted] addendum to UCDIRT notice #63. According to [redacted] "imapd" programs serve the same purpose as "statd" programs, that is, port mapping.

(U) (S) Likewise, another UCD administrator, [redacted] reviewed logs and discovered additional attempted "imapd" probes as early as November 18, 1997. The origin of these "imapd" probes appeared to be [redacted] Pages 1 and 2 of enclosure 1 is [redacted] addendum to UCDIRT notice #63.

(U) (S) Sacramento provided relevant UCD logs to the following:

1) [redacted] Columbia University, [redacted] administrator for bone.tc.columbia.edu.

2) [redacted] Harvard University, [redacted]

[redacted] administrator for scotia.harvard.edu.

3) [redacted] St. Andrews, [redacted] administrator for netgate.saes.com.

(U) (S) [redacted] provided pages 18, 19 and 20 of enclosure 1. [redacted] noted, SA [redacted] FBI Cleveland, [redacted] had also requested this information. SA [redacted] was contacted. SA [redacted] confirmed he was aware of Columbia's information, and had traced the intruder to [redacted] in [redacted] SA [redacted] was preparing to serve a search warrant on the subscriber. SA [redacted] was also advised the [redacted] intruder had successfully penetrated the UCD computer used for campus events and visitor services, had created a directory called /home/meta and a password entry name of [redacted] According to SA [redacted] this was the leitmotiv of his intruder. Pages 15, 16, and 17 of enclosure 1 were provided to SA [redacted]

(U) (S) [redacted] Harvard University, advised he had no logs for scotia.harvard.edu. [redacted] St. Andrews, likewise advised he had no logs for netgate.saes.com. However, [redacted] added he had been contacted by [redacted] University of Colorado-Boulder.

(U) (S) [redacted] University of Colorado-Boulder, [redacted] provided enclosure 2. [redacted] advised his network had been the target of a "statd" probe from netgate.saes.com, computer [redacted] The three compromised University of Colorado machines were all running Solaris 2.4+.

(U) (S) On 2/26/98, UCD Computer Security Analyst [redacted] was asked if the University had any indication their UCD machines had been used to launch flood attacks on any other computer networks. [redacted] said they had received a few complaints concerning some internet relay channels which had been flooded, but nothing else. On the other hand, [redacted] pointed out the UCD computers logged only TCP/telnet connections. Therefore, [redacted] did not believe UCD Administrators would be aware of any ping attacks launched from their networks. [redacted] added, UCD Administrators could track something other than standard TCP/Telnet connections only if the suspect activity occurred coincident with the tracking.

(U) (S) Sacramento is attempting to identify the subscriber who launched the "statd" probes from

To: NSD/CID From: Sacramento
Re: (U) ~~(S)~~ 288-HQ-1242560, 03/04/1998

[redacted] Any other leads will be left to the discretion of OSIIP/CITAC. b6 b7C

◆◆

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/02/98

[redacted] Academic Information Technology Services, University of Maryland, was interviewed telephonically from his place of employment located at the University of Maryland, College Park, MD 20742, telephone number [redacted] After being advised of the identity of the interviewing agent, [redacted] provided the following information:

[redacted] advised that the subscriber for the [redacted] account is a University of Maryland [redacted] who is an [redacted] at the University.

b6
b7C

[redacted] advised that in December of 1997, the University of Maryland system administrators noticed that someone was coming into the [redacted] account from overseas when they knew that [redacted] was in the United States. Consequently, [redacted] Academic Information Technology Services, sent an e-mail and spoke to [redacted] on January 16, 1998 advising her to change her password. [redacted] advised that on January 21, 1998, [redacted] changed her password. [redacted] advised that [redacted] does not recall if [redacted] was surprised when she was advised that her account had been compromised. Interview concluded.

Investigation on 03/02/98 at Falls Church, VA (telephonically)

File # 288-HQ-1242560 -169 Date dictated N/A

by [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

288-HQ-1242560
MAJ

The following investigation was conducted by Special Agent [redacted] b6 b7C

at Falls Church, VA

Attached are various news articles relating to the above captioned case.

288-HQ-1242560-170

ZDNN

NEED A NEW

ZDNet | News | Products | Internet | Shopping | Help! | Magazines
Downloads | Games | Mac | At Home | Learning | Community | Investor

Search ZDNN
Find It!

ZDNN Top News
Page One
News Bureau
Headline Scan
Internet Investor
Netdex Headlines
News Specials
News Archives

Sections
Business
Computing
Internet

Commentary
Rumors & Comment
Opinion Desk
Talk Back

ZDNN Radio
Headline News

Other News
PC Week Online
Interactive Week
Mac Week
Software Updates
Net Scouts

Services
Introduceds
Custom News
Company Finder
Headline Archive

Contact Us
The Staff

Magazines
PC Publications
International
Archive
Subscription

How the FBI tracked down alleged Pentagon hackers

By Rob Lemos, ZDNN
February 27, 1998 6:43 PM PST

The local hunt for the hackers who broke into 11 non-classified Pentagon computers began with a small provider in Santa Rosa, Calif.

"We originally detected the intrusions because the hackers made changes to our operating systems that were easily detectable," said Bill Zane, owner and operator of the 3,000-user Netdex Internet Services in Santa Rosa, Calif. "They were very sloppy in that respect." That was in mid-January.

In the weeks that followed, Zane worked with FBI agents and other network administrators in tracking down the trespassers. "After we figured out they were there, we could have closed up the security holes they were using," said Zane. "Instead, after reviewing the data and seeing the massive scope of it, we decided to take a risk and leave the door open for a while."

MUST SEE ZD

- **FBI's big crackdown nabs small-town teens.**
- **Poulsen: Why hack the Pentagon? Simple. Because it's there.**
- **CyberCrime Interrogation: Ken Geide, new No. 2 anti-hacking cop.**

In fact, "a while" turned into 6 weeks.

The entire time, the FBI kept their dogs on the electronic trail of what they thought could be

TOP STORIES

Updated February 28, 1998
9:58 AM PST

- FBI mounts big crackdown on small-town teens
- Bill to the hill
- No white knight seen for CSC
- HP secures crypto export

E-mail this!
Print this!

ZDNet's FREE Daily News & Investing E-mail alert!

potential terrorists. "The FBI had their 10 agents in San Francisco working on overtime over the last month," said Zane. "They considered this to be a very serious issue." Joining the local agent were others from the East Coast where most of the analysis was being done.

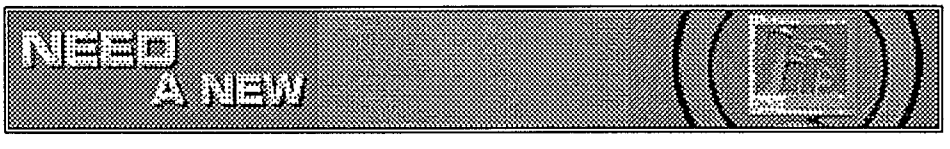
Zane, with system administrators from Massachusetts Institute of Technology and UC Berkeley, tracked the intruders and essentially "bugged" their communications. Those messages plus the different mode of operations lead Zane to believe someone is out there -- and they are an adult.

"The other methods were much more sophisticated and acted much more serious," he said.

Top

A ZDNet Site

ZDNET HOME | SITE MAP | SEARCH ZDNET | WHAT'S NEW | AD INFO | CONTACT US



ZDNN

Search on computer topic: (Virtual Reality) Go! COMPUTER MAGAZINE ARCHIVE

ZDNet | News | Products | Internet | Shopping | Help! | Magazines
Downloads | Games | Mac | At Home | Learning | Community | Investor

Search ZDNN
Find it!

ZDNN Top News
Page One
News Briefs
Headline Search
Internet World Report
Inside Headlines
News Search
News Discussion
Sections
Business
Computing
Internet
Commentary
Pointers & Comment
Anchor Desk
Talk Back
ZDNN Radio
Headline News
Other News
PC Week Online
Interactive Week
Mac Week
Computer News Daily
Net Politics
Services
Internet
Random News
Company Finder
Magazine Archive
Contact Us
The Staff
Magazines
US Publications
International
Archives
Subscriptions

FREE

Download Free!

So why hack the Pentagon? Simple. Because it's there

By Kevin Poulsen, ZDNN
February 27, 1998 6:48 PM PST

I was channel surfing last night when I caught the evening news, airing a clip from the 1983 movie *War Games*: Matthew Broderick typing on a keyboard, NORAD going on full alert, worldwide nuclear war looming.

I know what that means. Intruders have broken into yet another low-level Pentagon computer, and examined unimportant and unclassified information, all so they could win bragging rights with their friends.

Time to run for the bomb shelters.

MUST SEE ZD

- **FBI's big crackdown nabs small-town teens.**
- **Road to Cloverdale: How the FBI tracked down Pentagon hackers.**
- **CyberCrime Interrogation: Ken Geide, new No. 2 anti-hacking cop.**

At least one newspaper report suggested that the latest string of Defense Department hack attacks might be the work of the Iraqis. Well, Saddam can breathe a sigh of relief. It turns out the suspects are a couple of teenage hobbyists in Cloverdale, Calif. One of them is 15 years old.

The systems that were cracked housed personnel and payroll data. A Defense Department official characterized the intrusions as a "wake-up call" for increased computer security at the Pentagon. They've been getting this particular wake-up for 15

TOP STORIES
Updated February 28, 1998
9:58 AM PST

- FBI mounts big crackdown on small-town teens
- Bill to the hill
- No white knight seen for CSC
- HP secures crypto export

E-mail this!
Print this!

ZDNet's FREE Daily News & Investing E-mail alert!
SUBSCRIBE

years now, but someone keeps hitting the snooze button.

And with good reason.

The Defense Department has more computers than God and, as in any large bureaucracy, most of them are not very exciting. Classified systems are isolated from the outside world, physically and electronically and, when it comes to classifying data, the Pentagon errs on the side of caution.

So the only reason anyone would have for cracking a vulnerable Pentagon system is because it's there.

Should youthful adventurers be treated like serious saboteurs? Sadly, that's what is likely to happen ... after a lengthy investigation that will shadow the pranksters as they grow-up, get their first car, and register to vote for the first time.

If the Defense Department wanted to shore up security on its unclassified systems, they could have done it long ago. But then we'd miss the drama of G-men cordoning off a suburban street, and filing out of a *Brady Bunch* home with stacks of floppy disks and modems. We'd miss the chance to give the already-bloated Pentagon budget an extra billion for information security. We wouldn't get to pass new laws cracking down tighter on this grave threat to the American Way of Life.

And we'd never see the **War Games** clip again.

Depending on who you listen to Kevin Poulsen is either a misunderstood former hacker or a menace to society. He writes CHAOS Theory, a weekly column on the electronic underground for CyberCrime.

Top

A ZDNet Site

ZDNET HOME | SITE MAP | SEARCH ZDNET | WHAT'S NEW | AD INFO | CONTACT US

ZDNN

Search ZDNN
Find It!

ZDNN Top News
Page One
News Briefs
Headline Scan
Interactive Investor
Media Headlines
News Specials
News Elsewhere

Sections
Business
Computing
Internet

Commentary
Editor's Comment
Opinion Desk
Talk Back

ZDNN Radio
Headline News

Other News
PC Week Online
Interactive Week
Mac Week
Computer Retail Week
Net Profits

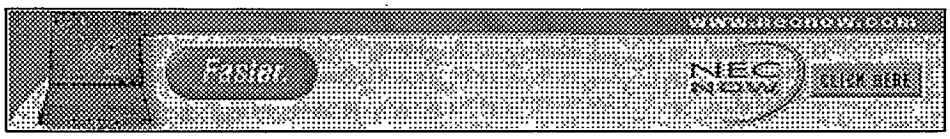
Services
Addresses
Custom News
Company Finder
Magazine Archive

Contact Us
The Staff

Magazines
US Publications
International
Archive
Subscription

Download FREE software!

Download Free!



FBI mounts big crackdown on small-town teens

By Robert Lemos, ZDNN
February 28, 1998 11:18 AM PST

The FBI spent six weeks and dedicated more than 20 agents to an effort to track down what it feared to be organized ring of intruders who cracked into Pentagon systems. But after two nighttime raids, the agency found itself dealing with the revelation late Friday that its intensive investigation may have nabbed nothing more than a couple of kids.

During one raid, the agents caught a teen, identified as a 15- or 16-year-old high-school student, in the process of breaking into a non-classified computer system. A second raid targeted the home of another youth suspected of taking part in the Pentagon hacks. The crackdown took place in Cloverdale, a town of some 5,000 residents about 100 miles north of San Francisco.

The two teenagers -- as minors -- were not arrested, but the FBI confiscated computer equipment and software in both homes.

MUST SEE ZD

- **Road to Cloverdale: How the FBI tracked down Pentagon hackers.**
- **Poulsen: Why hack the Pentagon? Simple. Because it's there.**
- **CyberCrime Interrogation: Ken Geide, new No. 2 anti-hacking cop.**

"These are good kids," said Michael Carey, superintendent of the Cloverdale Unified School District. "I'm betting that no charges will be brought against them"

TOP STORIES

Updated February 28, 1998
9:58 AM PST

- FBI mounts big crackdown on small-town teens
- Bill to the hill
- No white knight seen for CSC
- HP secures crypto export

E-mail this!
Print this!

RELATED LINKS

READ
RSA's encryption challenge solved in 39 days

Pentagon hack no surprise

Crypto Crew, Feds at Odds

ZDNet's FREE Daily News & Investing E-mail alert!

This ends a chapter in its investigation of several break-ins of unclassified Pentagon computers. The raid occurred the day after Deputy Defense Secretary John Hamre revealed that 11 unclassified Pentagon systems had been broken into earlier this month.

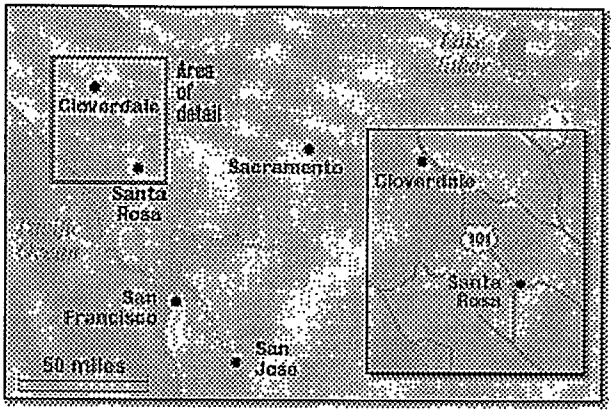
According to federal investigators, other Cloverdale High students are in the process of being questioned by Secret Service and FBI agents. The suspicion is that the hacking was being conducted by a ring of youths, who may have been in a contest to see who could get farthest into government computers.

"Most everyone here is thinking that this was some kind of computer contest" said one student at Cloverdale High School.

Earlier this week, Deputy Defense Secretary Hamre stated that the online trespasses were "the most organized and systematic attack the Pentagon has seen to date."

"This says amazing things about the kids' skills and really poor things about the Pentagon's security," said a hacker unrelated to the incidents, who preferred to be identified by his online name, darkcube.

But the hunt isn't over -- at least not according Bill Zane, who owns the 3,000-user Netdex Internet Services in Santa Rosa, Calif. The hackers apparently broke into Netdex on the way to the Pentagon. In fact, Zane may have given FBI agents their first bead on the intruders. "There's at least one more and most likely two more out there," Zane said. "It's not just these two kids."



Zane, with system administrators from Massachusetts Institute of Technology and UC Berkeley, tracked the intruders and essentially "bugged" their communications. Those messages plus the different mode of operations lead Zane to believe someone is out there -- and they are an adult.

"The other methods were much more sophisticated and acted much more serious," he said.

As for the two young hackers, worse crimes could have been committed. "I would have much more concerned if they had hacked the school system or tampered with grades," said Superintendent Carey. "It was more an innocent game than a malicious attack."

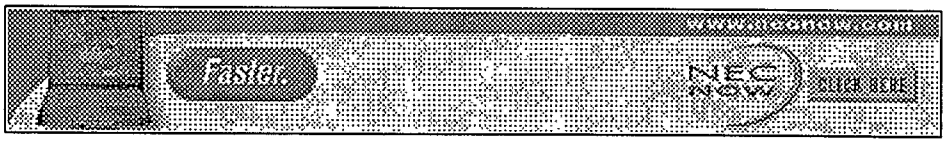
Alex Wellen, ZDTV CyberCrime, contributed to this report.

Top

ZDNN

A ZDNet Site

ZDNET HOME | SITE MAP | SEARCH ZDNET | WHAT'S NEW | AD INFO | CONTACT US



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

288-HQ-1242560
MAJ

The following investigation conducted by Special Agent [redacted]

at Falls Church, VA

An Internet news story attributed to "The Australian Online" dated October 21 1997, by [redacted] was obtained which indicates that [redacted] pleaded guilty to charges which carry a 10 year sentence. [redacted] plead guilty in Sydney District Court to the main offence under Section 76E of the Crimes Act for his hacking into an Australian ISP named AUSnet, changing their web page, and distributing their clients' credit card details across the Internet. Damages resulting from this incident are estimated to be $2 million. An additional eight charges are also indicated. [redacted] is reported to be sentenced in November 1997 for offenses related to other charges he faces on making $50,000 worth of illegal phone calls by tapping into the public telephone system. [redacted] hacker name is [redacted] and he is [redacted] years old. [redacted] is scheduled to be sentenced on February 5, 1998. A copy of this Internet news story is attached.

b6
b7C

A second Internet news story was obtained which also describes the legal status of [redacted] This story was contained in an email message dated 2/10/98 which was sent through an anonymous remailer. The story indicates the author to be [redacted] This story contains the following information: [redacted] of Sydney, Australia, is to be sentenced "today" for charges of hacking into the ISP AUSnet and circulating the information on 1200 credit cards onto the Internet. [redacted] faces a maximum 10 year sentence in the Downing Centre District Court. Damages estimated to be $2 million in lost clients and contracts. [redacted] hacked into AUSnet in March 1995, two months after he was refused a job with AUSnet. [redacted] faces 1 count of inserting data into a computer, which carries a maximum 10-year sentence, and 8 counts of unlawful access to computer data. A copy of this news story is attached.

288-HQ-1242560-173

the sign of a new PC experience.
Pentium® II processor click here

Optik Surfer faces 10 years for hack attack

By GEOFF LONG

October'21: Optik Surfer – the hacker who broke into the system of ISP AUSnet and distributed clients' credit card details across the Internet – has pleaded guilty to charges carrying a maximum penalty of 10 years imprisonment.

The Australian Federal Police computer crime unit spent more than six months in 1995 tracking down the hacker, who also altered the AUSnet Web site and sent e-mail messages from the system administrators' account. Computer crime agents spent almost 12 months preparing the case against the hacker.

Skeeve Stevens, a 27-year-old computer consultant, was charged with eight counts of gaining unlawful access to computer data and one count of inserting data into a computer system.

Stevens pleaded guilty in Sydney District Court to the main offence under Section 76E of the Crimes Act, which carries a 10-year sentence, and asked the court take the other eight charges into consideration when sentencing.

It is the second time in the past month that a hacker has pleaded guilty in court.

Next month another hacker will be sentenced for offences related to making up to $50,000 worth of illegal phone calls by tapping into the public telephone system.

Graham Henley, a former agent with the Australian Federal Police computer crime unit who now heads computer forensic services for Network Security Management, was involved in both cases.

Mr Henley tracked the source of the Optik Surfer attack to a computer laboratory at Monash University.

The court was told that after the break-in, the hacker returned to the system and sent an e-mail message to journalists from an account operated by AUSnet's technical director.

Identifying himself as the Optik Surfer, he boasted of his break-in and said that the credit card details had been distributed to highlight the poor security at AUSnet.

AUSnet's Web site was also altered to greet visitors with the quote: "Remember – too

many secrets."

The quote comes from Sneakers, a 1993 film about hackers starring Robert Redford.

Stevens originally denied being the hacker but claimed to the media that he was in contact with the so-called Optik Surfer.

Mr Henley was aware of Stevens as a result of a previous conviction for computer hacking.

Federal police alleged that Stevens' actions cost AUSnet more than $2 million in contract losses.

Banks had had to re-issue many of the credit cards.

The matter was adjourned for sentencing on February 5 next year.

TOP HOME

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

288-HQ-1242560
WME:wme wme

1

On March 5, 1998 [redacted] contacted Special Agent [redacted] by telephone. CS then furnished the following information:

CS discovered an online news article which includes an interview with the hacker named Analyzer. The address for this web page is http://www.antionline.com/PentagonHacker/HackerStory2.html. This is an interview conducted on an Internet chat service between Analyzer and another person using the name JP.

b6
b7C
b7D

SA [redacted] subsequently visited this Internet site and printed the interview. That material is attached to this insert.

288-HQ-1242560-176

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

288-HQ-1242560
MAJ

The following investigation was conducted by Special Agents (SA) [redacted] and [redacted]

at Falls Church, VA

On 02/19/98 [redacted] of Georgetown University, Computer Science Department, was interviewed at her place of employment, Georgetown University, Washington, DC 20057. SA [redacted] advised [redacted] that the [redacted] account at Georgetown University could have been compromised on 12/19/97 and 02/12/98. [redacted] advised that she would advise the system administrators of the Georgetown accounts of this information. b6 b7C

On 02/20/98 [redacted] advised SA [redacted] that the system administrator, [redacted] checked the [redacted] account. [redacted] advised that the [redacted] account did have any unusual logins on the dates that SA [redacted] provided. The 12/19/97 was a login from Georgetown University and the 02/12/98 login was a dial-up SLIP (Serial Line Internet Protocol) connection.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2012 BY [redacted]

288-HQ-1242560
MAJ

The following investigation conducted by Special Agent b6 b7C [redacted]

at Falls Church, VA b3 OTHER Sealed pursuant to court order

On 02/17/98, per [redacted] provided [redacted] (attached).

On 02/18/98, inquires to the NATIONAL CRIME INFORMATION CENTER (NCIC) INTERSTATE IDENTIFICATION INDEX (III) were negative regarding any criminal identifiable with [redacted] Date of Birth [redacted]

On 02/18/98 inquires to the VIRGINIA DEPARTMENT OF MOTOR VEHICLES disclosed the following information regarding [redacted] Date of Birth [redacted]:

[redacted]

b6
b7C

On 02/18/98 inquires to the MARYLAND DEPARTMENT OF MOTOR VEHICLES disclosed no record regarding [redacted] Date of Birth [redacted]

On 02/18/98, inquiries to the LEXIS-NEXIS PERSON LOCATOR database disclosed the following regarding [redacted] permanent address, [redacted]

RESIDENT(S)	APPROXIMATE BIRTH DATE
[redacted]	

288-HQ-1242560-179

[redacted]

On 02/18/98, inquiries to the LEXIS-NEXIS PERSON LOCATOR database disclosed the following names listed with [redacted] local address, [redacted] which is a [redacted] dwelling:

[redacted]

b6
b7C

On 02/18/98 inquires to the AUTOMATED CASE SUPPORT (ACS) system disclosed negative results regarding [redacted]

On 03/02/98 [redacted] FBIHQ, made an inquiry to the IMMIGRATION AND NATURALIZATION (INS) database located at FBIHQ, National Security Division, and advised that there is no record of [redacted] in the INS database.

~~SECRET~~

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

0-93 (Rev. 01/25/91)

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
COMMUNICATION MESSAGE FORM

TRANSMIT VIA:
☒ Teletype

PRECEDENCE:
☒ Immediate
☐ Priority
☐ Routine

CLASSIFICATION:
☐ TOP SECRET
☒ ~~SECRET~~
☐ CONFIDENTIAL
☐ UNCLAS E F T O
☐ UNCLAS

DATE: 3/5/98

^PAGE 1 OF 6

FM DIRECTOR FBI 288-HQ-1242560

TO TEL AVIV/LEGAT ATHENS/IMMEDIATE/

FBI HOUSTON/IMMEDIATE/

FBI SAN FRANCISCO/IMMEDIATE/

FBI WASHINGTON FIELD/IMMEDIATE/

BT

~~SECRET~~

CITE: //1312//

PASS: ATHENS PASS TO LEGAL ATTACHE TEL AVIV; SPECIAL AGENT IN CHARGE (SAC) HOUSTON; SAC SAN FRANCISCO; SAC WASHINGTON FIELD.

SUBJECT: SOLAR SUNRISE; CITA MATTES; OO: HQ.

(U) ~~(S)~~ TEL AVIV IS TO MAKE NO OVERT INQUIRIES CONCERNING THIS MATTER, RELEASE ANY INFORMATION, NOR INDICATE THIS INVESTIGATION IS PENDING TO ANY FOREIGN OR ISRAELI GOVERNMENT INDIVIDUAL OR REPRESENTATIVE. [redacted]

Referral/Consult

288-HQ-1242560-181

******* FOR COMM CENTER USE ONLY *******

NOTE: Copy Designations Are On The Last Page Of This Teletype!!!

Approved By DAG

MRI/JUL 595/0641

Transmitted 15122 [redacted] MAR 05 1998

ISN 010

DTG 050150Z MAR 98

~~SECRET~~

b6
b7C

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
COMMUNICATION MESSAGE FORM

Referral/Consult

[redacted]

(U) [redacted] ~~(S)~~ ON FEBRAURY 25, 1998, FBI-SF EXECUTED TWO SEARCH WARRANTS AT RESIDENCES OF TWO JUVENILE MALES IN [redacted] CALIFORNIA. ONE OF THESE JUVENILES, KNOWN AS [redacted] HAD INTERNET CHAT CONVERSATIONS WITH [redacted] WAS COACHING [redacted] ON HOW TO HACK SYSTEMS. [redacted] CLAIMS TO BE [redacted]

b6
b7C

MORE INFORMATION WILL FOLLOW; HOWEVER, TEL AVIV SHOULD BE ADVISED THAT POSSIBLE CONTACT WITH ISRAELI LAW ENFORCEMENT MAY BE

(U) REQUESTED. ~~(S)~~ FBIHQ IS ACTING AS OO IN THIS MATTER. ANY INFORMATION SHOULD BE DIRECTED TO THE CASE AGENT, SSA [redacted]

~~SECRET~~

0-93A (Rev. 01/25/91)

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
COMMUNICATION MESSAGE FORM

^PAGE 6 ~~SECRET~~

[redacted] VIA SECURE VOICE [redacted] OR SECURE FACSIMILE [redacted] TEL AVIV IS INSTRUCTED TO CHECK OPEN SOURCE INFORMATION, INCLUDING RECENT NEWSPAPER ARTICLES, FOR REFERENCES TO COMPUTER HACKING OF THE ISRAELI KNESSET AND TELEPHONE SYSTEM. ALSO CHECK FOR REFERENCES TO [redacted] AND THE "ISRAELI INTERNET UNDERGROUND". DETERMINE [redacted] HOME ADDRESS, CRIMINAL HISTORY, AND OTHER RELEVANT BACKGROUND.

b6
b7C

~~CLASSIFIED BY: 4511, CITAC/D5~~
~~REASON: 1.5 (C)~~
~~DECLASSIFY ON: X-1~~

BT

////

~~SECRET~~

~~SECRET~~

DRAFTED BY: HEB:MAC ROOM: 11887 EXT: [redacted]

COPY COUNT:

1 - [redacted]

1 - MR. GEIDE

1 - [redacted]

1 -

1 -

b6
b7C

APPROVED:

Director	Crim. Inv.	Inspection	Training
Deputy Director	CJIS	Laboratory	Off. of EEO Affairs
	Finance	National Sec.	Off. of Public & Cong. Affs.
	Gen. Counsel	OPR	
	Info. Res.	Personnel	

~~SECRET~~

(01/26/1998)

DECLASSIFIED BY [redacted]
ON 09-24-2012

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/13/1998

To: Jacksonville **Attn:** Ft. Walton Beach RA
Jacksonville **Attn:** Panama City RA

From: Jacksonville
Squad 5
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-HQ-1242560 (Pending) - 182

Title: (U) SOLAR SUNRISE;
CITA MATTERS;
OO: HQ

Synopsis: (U) ~~(S)~~ To set forth detailed leads with regard to possible computer intrusions at U. S. Air Force (USAF) installations.

(U) ~~(S)~~ ~~Classified By: 4511, CITAC/D5~~
~~Reason : 1.5(c)~~
~~Declassify On: 02/12/2008~~

Reference: (U) ~~(S)~~ 288-HQ-1242560 Serial 52

Enclosures: (U) Enclosed for Ft. Walton Beach and Panama City RAs are one (1) copy each of referenced communication.

Details: (U) ~~(S)~~ In early February, 1998, the Department of Defense began detecting intrusions into its unclassified computer systems at various U. S. facilities. The method and means of the intrusions are described in detail in referenced EC. FBIHQ is seeking to identify any additional intrusions which may be ongoing or as yet unknown. Accordingly, the following leads are set forth with regard to USAF installations within the territory of the Jacksonville Division.

(U) Lead #1 for Jacksonville in referenced communication is considered covered.

~~SECRET~~

To: Jacksonville From: Jacksonville
Re: (U) ~~(S)~~ 288-HQ-1242560, 03/13/1998

LEAD (s):

Set Lead 1:

JACKSONVILLE

AT FORT WALTON BEACH (EGLIN AFB), FLORIDA

(U) ~~(S)~~ Contact System Administrator or other individual in charge of computer system security at Eglin Air Force Base. Determine whether any intrusions of the nature described in referenced EC have occurred. Furnish any positive results to SSA [redacted] or SSA [redacted] FBIHQ, [redacted] b6 b7C

Set Lead 2:

AT FORT WALTON BEACH (HURLBURT FIELD), FLORIDA

(U) ~~(S)~~ Contact System Administrator or other individual in charge of computer system security at Hurlburt Field Air Force Base. Determine whether any intrusions of the nature described in referenced EC have occurred. Furnish any positive results to FBIHQ as above.

Set Lead 3:

AT PANAMA CITY, FLORIDA

(U) ~~(S)~~ Contact System Administrator or other individual in charge of computer system security at Tyndall Air Force Base. Determine whether any intrusions of the nature described in referenced EC have occurred. Furnish any positive results to SSA [redacted] or SSA [redacted] FBIHQ, [redacted] b6 b7C

♦♦

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/11/1998

To: National Security/CID **Attn:** CITAC/Rm 11887
SSA [redacted]

From: Springfield
Fairview Heights RA
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :lms

Case ID #: (U) ~~(S)~~ 288-HQ-1242560-183 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO: HQ;

[redacted]

(U) ~~(S)~~ ~~Classified By: 4511, CITAC/D5~~
~~Reason : 1.5(c)~~
~~Declassify On: 02/12/2008~~

Reference: (U) ~~(S)~~ 288-HQ-1242560 Serial 52 Referral/Consult

[redacted]

[redacted]

~~SECRET~~

Rm 11887

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

439

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/10/1998

To: WFO **Attn:** SSA [redacted]

From: FBIHQ
OCIIP/CITAC/CIU
Contact: A/UC [redacted]

Approved By: Geide Kenneth M [redacted]

Drafted By: [redacted]:drn

Case ID #: [redacted]ending)
288-HQ-1242560-188 Pending)

b6
b7C
b7E

Title: INFILTRATION OF MILITARY
COMPUTER SYSTEMS

Synopsis: This communication directs WFO to Open and Assign a case involving the compromise of multiple military computer systems.

Details: Reference telcall between A/UC [redacted] and SSA [redacted] dated 2/10/98.

In referenced telcall, it was agreed that WFO would Open and Assign a case involving the penetration of multiple military computer systems from CLARK.NET and IAPNET.COM. This case is currently being worked by the Naval Criminal Investigative Service (NCIS). NCIS has identified a possible subject in Jacksonville, FL. The subject is believed to be a student at the University of North Florida.

WFO has been assigned responsibiity for the Jacksonville territory per 7/16/96 EC to all Field Offices.

Uploaded by SDH 2/3/98

CLA 2/3/98

LEAD (s):

Set Lead 1:

WFO

AT WFO

Open and Assign this matter in order to assist with the debriefing of possible subject in Florida.

♦♦

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

439

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/23/1998

To: FBI Headquarters ✓ Attn: NIPC/CIU/Room 11887
SSA [redacted]

San Francisco Attn: CITA Squad, 14B

From: WFO
Squad C-17/NVRA
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :wme wme

Case ID #: 288-HQ-1242560 (Pending) -191

Title: SOLAR SUNRISE;
CITA MATTERS;
OO: HQ

Synopsis: Lead set for information requested from DISA/ASSIST.

Details: On 3/23/98 WFO Squad C-17 received a telephonic request from DISA / ASSIST for information regarding previously unknown victims of intrusions by the hacker named [redacted] Recent news reports have described [redacted] as having compromised as many as 400 government computers in the United States. DISA / ASSIST has requested that, if such information was obtained by investigators following the recent arrest of [redacted] DISA would like a list of the allegedly compromised military computer systems. As it is the responsibility of DISA / ASSIST to address such intrusions, they are interested in (1) confirming any reported compromises to any U.S. military computer systems, and (2) assisting in repairing any confirmed compromises to those systems. b6 b7C

DISA / ASSIST expressed concerned that [redacted] may have shared such information with other hackers, since [redacted] is known to operate with a group of hackers. Other hackers might exploit the information by attacking vulnerable military computer systems. For this reason, it is requested that NIPC respond to this request by 04/10/98.

Assistance from FBIHQ is requested in addressing this request.

This is being furnished to San Francisco for information only.

[redacted] b6 b7C

Responded to on 5/20/98

To: FBI Headquarters From: WFO
Re: 288-HQ-1242560, 03/23/1998

LEAD (s):

Set Lead 1:

FBI HEADQUARTERS

AT WASHINGTON DC

Request NIPC/CIU confirm whether investigation has identified large numbers of allegedly compromised computer systems, as reported by [redacted] in public news sources. If available, WFO requests NIPC to furnish WFO with information identifying allegedly compromised hosts which are on U.S. military networks (.mil). WFO will transmit this information to DISA / ASSIST enabling them to address this matter by: confirming the alleged compromises, and repairing those compromised hosts.

b6
b7C

DISA / ASSIST is concerned that [redacted] may have shared such information with other hackers, who might exploit the information by attacking vulnerable military computer systems. For this reason, it is requested that NIPC respond to this request by 04/10/98.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

459

[rev 3/3/98]

National Infrastructure Protection Center (NIPC)

date _____

TO	ROOM	NAME
____	7142	[redacted]
____	7116	
____	7110	
____	7110	
____	7443	
____	4012	
____	4012	
____	11741	
____	11887	
____	4825	
____	5849	
____	5222	
____	11887	
____	11887	
____	11887	
____	11887	

TO	ROOM	NAME
____		Strategic Planning Analysis Unit Acting UC [redacted]
____		Computer Investigations Unit Acting UC [redacted]
____		Special Technologies Applications Unit UC [redacted]
____		Criticial Infrastructure Protection Unit UC [redacted]
____		Watch and Threat Analysis Office Acting UC [redacted]
____		[redacted]
____	7975	[redacted]
____		[redacted]
____		[redacted]
____	Room	

b6
b7C

please file in Solar Sunrise
4.6.98

COMMENTS [redacted] – DoJ Exec. Sec. should not have sent this back to us. I've talked to [redacted] re this, this office, and he will take care of it (can you send the original back to him on Friday (but put a copy in my S.S. Sunrise file with this note), and tell the Exec. Sec. to amend their records to show that the FBI will send this kind of thing directly to the lead agency? Thanks! CAG

____ Please Call Me
____ Please Discuss with Me
__✓__ Appropriate Action

____ For Your Information
____ For Your Approval
____ Please Prepare Response

MV

MICHAEL A. VATIS
Chief, Deputy Assistant Director
Room 11887, Ext. 0307

288-HQ-1045560-197

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

To: NATIONAL SECURITY DIVISION FO b6 Control No. 500767
Room: 7110 Name: [redacted] b7C

Date Received: 03/31/98 DOJ Due Date: 04/02/99

FBI CENTRAL REGISTRY
EXECUTIVE SECRETARIAT
CORRESPONDENCE MANAGEMENT SYSTEM
Room 6242, Ext 6014

Instructions:

The attached has been assigned to your Unit and should be finalized before the due date shown above.

If this matter needs to be reassigned to another entity, the FBI Central Registry (CR) should be advised immediately. The CR will need to know to whom request was reassigned, together with room and telephone numbers and contact point.

All responses are to be routed to the DOJ Executive Secretariat by the CR; therefore, the entire package should be sent to Room 6242. A copy of all outgoing correspondence MUST be designated for the FBI Central Registry (FBICR), Room 6242. This copy must contain a copy of the control sheet or the Executive Secretariat control number since the CR must close out all requests. An additional copy is required for Executive Secretariat, DOJ, Room 4400AA, as instructed on the ES control sheet. These copies should appear as:

1 - Exec Sec, DOJ, Room 4400AA - Encs.
1 - OLA, DOJ, Room 1612 - Enc.
1 - FBICR, Room 6242 - Enc. (or Control #)

RETURN ENTIRE PACKAGE TO ROOM 6242

DO NOT SEND TO MAILROOM

Department of Justice
EXECUTIVE SECRETARIAT
CONTROL SHEET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

1. FOLDER No: 500767
2. TRACKING ID No: X98-036690
3. RESERVED
4. DATE OF DOCUMENT: 03/20/98
5. DATE RECEIVED: 03/23/98
6. DUE DATE: 04/02/98

7. FROM: Louis J. Freeh
Director
Federal Bureau of Investigation
Washington, DC 20535

8. TO: AG

9. CATEGORY: MEM-ACTION

10. SUBJECT:
Memo regarding items proposed for dissemination to the NSC. Provides an update on two cases in which the NSC has expressed an interest. See folders 498180, 498136 & 486197. Attachments. See folder 502036.

11. ACTION/INFORMATION:

Referred To:	Date Assigned:	Action:
ESFILES	03/31/98	For closing, filing, and dispatching. AG approved and signed on 3-30-98 by OAG. Original forwarded to FBI for handling.
OAG	03/26/98	For AG decision. For AG approval/disapproval.
ODAG	03/24/98	For DAG initialing on Action Memorandum. Return to Executive Secretariat for forwarding to AG. 3/26/98: DAG initialed on 3/25/98.

Referred To:	Date Assigned:	Information:

12. RESERVED FOR EXECUTIVE SECRETARIAT USE
AG FILE: FEDERAL BUREAU OF INVESTIGATION General AG Chron AS-3-30-98
: NSC interest in 2 FBI cases

13. EXECUTIVE SECRETARIAT CONTACT: [redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

b6
b7C

U.S. Department of Justice

Federal Bureau of Investigation

March 20, 1998

MEMORANDUM FOR THE ATTORNEY GENERAL

THROUGH: THE DEPUTY ATTORNEY GENERAL

FROM: DIRECTOR, FBI

SUBJECT: ITEMS PROPOSED FOR DISSEMINATION
TO THE NATIONAL SECURITY COUNCIL

PURPOSE: To provide a letterhead memorandum with an update on two cases in which the National Security Council, (NSC) has expressed an interest.

TIMETABLE: None.

SYNOPSIS: The NSC has expressed an interest in the facts of the "Solar Sunrise" and "Blue Retina" investigations. The attached memoranda are appropriate for dissemination to the NSC, via White House Counsel, at your discretion.

DISCUSSION: The NSC has expressed an interest in obtaining information about two pending FBI cases captioned, "SOLAR SUNRISE" and "BLUE RETINA." Consistent with the Department of Justice procedures governing communications with the White House about pending criminal and civil investigations, it is left to your discretion to forward the attachments to the White House Counsel for dissemination to the National Security Council, as appropriate.

RECOMMENDATION: That the Attorney General provide the White House Counsel with the aforementioned information for dissemination to the NSC, as appropriate.

APPROVE [redacted] b6 b7C

DATE March 30, 1998

Concurring Components:

None

DISAPPROVE _____

Nonconcurring Components:

None

OTHER _____

Enclosures (2)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 20,1998

SOLAR SUNRISE

This case involves intrusions into military, government, educational, and commercial computers. The intrusions were made by exploiting a known vulnerability inherent in certain operating systems. This exploit is called, "STATD," pronounced stat-dee. While this exploit has been seen throughout the network community for approximately one year, a significant increase in observations was observed in certain military and government network systems beginning in mid-January 1998.

On February 3, 1998, the Air Force Computer Emergency Response Team (AFCERT) notified the National Infrastructure Protection Center at FBI Headquarters of these intrusions. As a result, a joint investigation was initiated. That investigation quickly centered upon three individuals. Two of those individuals reside in California. Both of these subjects are juveniles. The third individual is an [redacted] year old who resides in Israel. b6 b7C

On February 25, 1998, agents from the FBI's San Francisco office and agents from Air Force Office of Special Investigations (AFOSI), and Naval Criminal Investigative Services (NCIS) conducted a search of the residences of the two California residents. The search was conducted pursuant to a search warrant. The search warrant was based in part upon interceptions of data made pursuant to a court-ordered data wiretap. During the search, the two subjects were interviewed in the presence of their parents. Both confessed to their participation in the intrusions. Both also provided information regarding the Israeli subject.

NOT APPROPRIATE FOR DISSEMINATION TO THE PUBLIC

Re: Solar Sunrise

On March 14, 1998, agents from the FBI, AFOSI, and the National Aeronautics and Space Administration - Office of the Inspector General (NASA - OIG) traveled to Israel in order to secure the assistance of the [redacted] in procuring evidence necessary for a successful prosecution of the Israeli citizen. As a result, on March 18, 1998, [redacted] b6 b7C b7D

[redacted]

[redacted] b6 b7C b7D

Federal agents remain in Israel to assist in the debriefing of all subjects involved. It is our intent to obtain sufficient evidence to prosecute this matter in the United States in the unlikely event that Israel agrees to extradite these individuals.

Department of Justice
EXECUTIVE SECRETARIAT
CONTROL SHEET

1. FOLDER No: 498180
2. TRACKING ID No: X98-034339
3. RESERVED
4. DATE OF DOCUMENT: 03/18/98
5. DATE RECEIVED: 03/19/98
6. DUE DATE: No Due Date

7. FROM: Mark M Richard
Deputy Assistant Attorney General
Criminal Division
Washington, DC 20530

8. TO: AG/DAG

9. CATEGORY: URGENT-RPT

10. SUBJECT:
Urgent Report advising that recently a U.S. investigative team traveled to Israel to pursue the DOD hacking case against the Israeli known as [redacted] a co-conspirator and hacking tutor of one of the CA teenagers previously searched for hacking military and civilian systems. CRM/Richard discussed this case [redacted] See 498136 & 486197. (ehz)

b6
b7C
b7D

11. ACTION/INFORMATION:

Referred To:	Date Assigned:	Information:
OAG	03/19/98	For information. Limited Distribution. To AG, OAG (Hogan).
ODAG	03/19/98	For information. Limited Distribution. To DAG/EONS, ODAG (Litt).
PAO	03/19/98	For information. Limited Distribution.

12. RESERVED FOR EXECUTIVE SECRETARIAT USE
See 497605, 500767. [redacted] DOD computer hacking

b6
b7C

13. EXECUTIVE SECRETARIAT CONTACT: [redacted]

Department of Justice
EXECUTIVE SECRETARIAT
CONTROL SHEET

1. FOLDER No: 498136
2. TRACKING ID No: X98-034292
3. RESERVED
4. DATE OF DOCUMENT: 03/18/98
5. DATE RECEIVED: 03/18/98
6. DUE DATE: No Due Date

7. FROM: John C. Keeney
Acting Assistant Attorney General
Criminal Division
Washington, DC 20530

8. TO: AG/DAG

9. CATEGORY: URGENT-RPT

10. SUBJECT:
Urgent Report regarding the arrest in a DOD hacking case against an Israeli known as the ``[redacted]`` See folder 486197. (cah) See folder 498180. b6 b7C

11. ACTION/INFORMATION:

Referred To:	Date Assigned:	Information:
OAG	03/18/98	For information. Limited Distribution. To AG, OAG (Hogan).
ODAG	03/18/98	For information. Limited Distribution. To DAG/EONS, ODAG (Litt).
PAO	03/18/98	For information. Limited Distribution.

12. RESERVED FOR EXECUTIVE SECRETARIAT USE
DOD hacking case

13. EXECUTIVE SECRETARIAT CONTACT: [redacted] b6 b7C

Department of Justice
EXECUTIVE SECRETARIAT
CONTROL SHEET

1. FOLDER No: 486197
2. TRACKING ID No: X98-024789
3. RESERVED
4. DATE OF DOCUMENT: 02/26/98
5. DATE RECEIVED: 02/27/98
6. DUE DATE: No Due Date

7. FROM: Michael J. Yamaguchi
U.S. Attorney, N.D. of California
San Francisco, CA 94102

8. TO: AG/DAG

9. CATEGORY: URGENT-RPT

10. SUBJECT:
Urgent Report advising that on 2/25/98, the FBI executed search warrants and seized computers and computer storage devices. The subjects admitted their illegal entries into computer systems which included some military computers. (Note: EOUSA e-mailed ODAG and CRM.) (ehz)

11. ACTION/INFORMATION:

Referred To:	Date Assigned:	Information:
CRM	02/27/98	For information. Limited Distribution. cc indicated for CRM (Charney).
OAG	02/27/98	For information. Limited Distribution. To AG, OAG (Hogan).
ODAG	02/27/98	For information. Limited Distribution. To DAG, ODAG (Litt).
PAO	02/27/98	For information. Limited Distribution. cc indicated for PAO ( ).

12. RESERVED FOR EXECUTIVE SECRETARIAT USE
AG FILE: REPORTS DOJ Urgent Sensitive
: #2489 - FBI search warrants, illegal computer system entries

b6
b7C

13. EXECUTIVE SECRETARIAT CONTACT:

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/05/1998

To: WMFO

From: National Security Division
National Infrastructure Protection Center
Contact: [redacted]

Approved By: [redacted]
Geide Kenneth
[redacted]

b6
b7C

Drafted By: [redacted]:cfs

Case ID #: ~~HQ-288-1242560~~ 288-HQ-1242560-199

Title: CHAIN OF CUSTODY FOR
UNIVERSITY OF MARYLAND EVIDENCE
SOLAR SUNRISE

Synopsis: Clarification of the chain of custody for evidence obtained from the University of Maryland in support of SOLAR SUNRISE.

Details: On March 2, 1998 at 10:50am [redacted] received the evidence from [redacted] (Block 11). On that same day [redacted] delivers evidence to [redacted]/CART who accepts evidence at 12:10pm (Block 12). [redacted]/CART began to fill out Block 13 but deletes his signature (Block 13). [redacted] under the false impression she needs to sign a second time for the release of the evidence completes Block 15 leaving Block 14 empty. [redacted] accepted the evidence and records his acceptance in Block 16. [redacted] incorrectly enters the time and date in Block 16. [redacted] latter corrected this error and initialed the changes. [redacted] accepted the receipt of evidence on 3/3/98 at 9:45am filling out the only remaining empty block (Block 14). [redacted] aware that the chain of custody appears confusing labels block 14 "A" and in the remarks section repeats his acceptance of evidence with date and time.

b6
b7C

♦♦

uploaded
by arj
4/7/98

CHAIN OF CUSTODY

Item	Accepted Custody	Date	Time	Released Custody	Date	Time
	Signature [redacted] Reason COLLECTED EVIDENCE	2/18/98	9:30A	Signature [redacted] Reason TURNED OVER TO CASE AGENT	2/18/98	11:32A
	Signature [redacted] Reason review data	2/18/98	11:33A	Signature [redacted] Reason release to evid	2/19/98	1:20pm
	Signature [redacted] Reason Storage	2/19/98 1:21 PM		Signature [redacted] Reason CART PROCESSING	2/19/98 1:22P	1:22P
	Signature [redacted] Reason CART Processing	2/19/98 3:00P		Signature [redacted] Reason [redacted]	2/20/98 2001	
	Signature [redacted] Reason Collected tapes	2/20/98 3:30p	3:30 pm	Signature [redacted] Reason Return to Evidence	2/27/98 2:05	2:05 pm
	Signature [redacted] Reason CART Confirmation	3/2/98 10:50AM	BLOCK 12 10:50AM	Signature [redacted] Reason CART Confirmation	3/2/98	12:10PM
BLOCK 13	Sig [redacted] Reason [redacted]	[redacted] [redacted]	BLOCK 14 A	Signature [redacted] Reason Pickup from CAR	3/3/98	9:45 AM
BLOCK 15	Signature [redacted] Reason released to examiner	3/2/98 1230pm	BLOCK 16	Signature [redacted] Reason Cart	3-2-98 ~~3-3-98~~ 1240 ~~900~~	

REMARKS Block A [redacted] received from [redacted] at 9:45am 3/3/98

3/4/98 8:30a [redacted] to deliver to WFO

3/4/98 12:40p [redacted] deliver to storage

Referral/Consult

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

Control of General/Drug/Valuable Evidence
FD-192 (Rev. 1-5-89)

Date 2/18/98

☒ General Evidence ☐ Drug Evidence ☐ Valuable Evidence

☒ Special Handling Requirement (i.e., FBI Lab Instructions Re Body Fluid Stains, Whole Blood, etc.)

MAGNETIC MEDIA KEEP AWAY FROM MAGNETS & ELECTRIC MOTORS

Title and Character of Case

SOLAR SUNRISE;
CITA MATERS;

FILE NO. 288-HQ-1242560

OO: HQ

Date Acquired	Acquired From:
2/18/98	[redacted], SOFTWARE ENGINEER, U OF MD

b6
b7C

To Be Returned	See Serial	Acquiring Agent	Case Agent
☐ Yes ☒ No		SA [redacted]	SSA [redacted]

☐ Yes ☒ No Grand Jury Material - Disseminate Only Pursuant to Rule 6(e), Federal Rules of Criminal Procedure

☐ Yes ☒ No Property To Be Forfeited To The U.S. Government

Description of Property (Be Specific)

HEWLETT PACKARD DDS 2 DIGITAL DATA STORAGE MEDIA RECOGNITION SYSTEM 4MM 120 METER DATA CARTRIDGE LABELED: 120 METER 148 W/INITIALS KH TJM DATED 2/18/98.

FOR DRUG AND/OR VALUABLE EVIDENCE ONLY - NAMES OF TWO AGENTS INITIALLY VERIFYING AND SEALING:

For Use By ECT:

Location of Property:

Control Number:

(File Copy)

BLOCKSTAMP

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/06/1998

To: FBIHQ Attn: ✓CITAC, SSA [redacted]

From: WFO
C-17
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :maj

Case ID #: ✓288-HQ-1242560 (Pending) -301

Title: SOLAR SUNRISE;
CITA

Synopsis: Lead coverage pending FBIHQ/WFO coordination with [redacted] [redacted] GTE. b6 b7C

Details: On 03/06/98 [redacted] for GTE, was interviewed telephonically regarding the [redacted] [redacted] advised that GTE would like to cooperate; however, GTE's legal department requires a subpoena before [redacted] can release the data to the FBI. [redacted] advised that he informed SSA [redacted] of this requirement. WFO is coordinating this matter with FBIHQ. b3 b6 b7C

Investigation conducted regarding [redacted] and the use of gospelcom.net, thegospel.net, and slip-stream.net. Gospelcom.net sells religious items on their webpage and was not contacted due to [redacted] associated with the site. Thegospel.net did not respond to multiple telephone messages. Slip-stream.net was contacted and advised that they did not see anything unusual, have been hacked before, and consider this as part of doing business. WFO believes that [redacted] is not related to the above captioned case. b6 b7C

Investigation is being conducted into [redacted] and is being coordinated with Naval Criminal Investigative Service (NCIS). A separate investigation was opened as [redacted] Case Agent [redacted] b3 b6 b7C

Investigation conducted re the [redacted] Two 2703d court orders and one supplemental 2703b order were served to [redacted] to the [redacted] account is [redacted] b7E

[redacted] Per the trap and trace order, [redacted]

[redacted]

b3
b6
b7C

Investigation conducted into [redacted] and opened as 295B-WF-211285, Case Agent [redacted]

b6
b7C
Referral/Consult

♦♦

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2012 BY [redacted]

439

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/06/1998

To: FBIHQ Attn: CITAC, SSA [redacted]

From: WFO
C-17
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :maj

Case ID #: 288-HQ-1242560 (Pending) -202

Title: SOLAR SUNRISE;
CITA

Synopsis: Leads covered.

Details: 1. All logical sources were contacted for information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating system. Results negative.

2.1. Two 2703d court orders and one supplemental 2703b order were served to [redacted] in order to determine [redacted] b3 b7E

2.2 . Contact established with DISA. Investigation conducted into the suspected role of [redacted] and the use of gospelcom.net. WFO believes that [redacted] is not related to the above captioned case. b6 b7C

2.3. Separate investigation opened into [redacted] in coordination with the investigation with Naval Criminal Investigative Service (NCIS), focusing on the intrusions that occurred at the U.S. Naval bases. Case [redacted] Case Agent [redacted] b6 b7C b7E

Unless further advised, WFO considers these leads RUC.

♦♦

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

439

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 04/02/1998

To: ✓FBI Headquarters Attn: SSA [redacted]
NIPC, Room 11887

From: WFO
Squad C-17, NVRA
Contact: SA [redacted] b6 b7C

Approved By: [redacted] SSA

Drafted By: [redacted] JJ 21

Case ID #: 288-HQ-1242560 - 204 (RUC)

Title: Solar Sunrise;
CITA

Synopsis: FD-302's enclosed re 3/11/98 interview of [redacted] WFO considers this matter RUC.

Enclosures: Enclosed for FBIHQ are two copies of an FD-302 detailing a 03/11/98 interview of [redacted] re the above captioned matter.

Details: On 02/17/98 and 03/11/98 interviews of [redacted] were conducted regarding the above captioned matter and Case ID # 295B-WF-211285, an IPR matter. Referral/Consult

FD-302's documenting the 02/17/98 interview have been previously forwarded to FBIHQ.

Subsequent to the 03/11/98 interview, [redacted] regarding this matter.

Inasmuch as all investigation conducted by WFO and [redacted] has yielded no evidence linking [redacted] to the above captioned matter, WFO will conduct no further investigation and considers this matter RUC.

◆◆

11887

b6 b7C

288-HQ-1242560-204

[redacted]

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

1-1

floppy disc w/ the ~~database~~ get a copy
to import into a database - [redacted]

where is the info. coming from.

[redacted] NS 2C AmDocs.
[redacted] NS 2B Iraq
NS 1 Russia
Denmark 203 Class.
[redacted]
Japan & Okinawa

b6
b7C

florida [redacted]

International Unit

Names sent by INS in Notebook
Microsoft Applicatin

Last Entry stud > quick finder to
find names

No organizatin

288-HQ-1242560
288 HQ-1242560-207
fm: [redacted]

no matches on list of schools.
ENCLOSURE -

to: [redacted] 2/14/98

DOC LAB NOTE

ENVELOPE

EMPTY

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

431 (1)

2703 (d)
agencies to making contacts

[redacted]

Relevant Sites

b3
b6
b7C
b7E

maybe rep. case.

SF

USSS

to wfo possible

subj. identified at ↓ UNF (IK)

[redacted]

[redacted]

Consensual - [redacted] OL

Pertinent Sites

b3
b6
b7C
b7E

Banner ← currently have 3 viable launching pad for attack putting tap and trace

[redacted]

USR → GREP

adoia

ftp

enclosed 288-HQ-1242560-28

288-HQ-1242560

from: ctac
to: ctac
2/14/98

Issues

RFI flag → for [redacted]

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

to be determined

future search data warrant

Issues

Logs

DISA get copies

Process

- [redacted] Referral/Consult

copy admin logs → logs → here Bart copies to [redacted] for processing & for process back post process back to us for leads

Cart
Solaris system
Tape Drives
DP, TAR

coordinating w/ [redacted]

assistance w/ personnel to WFO

of Navy DISA

Copies of Data

Major offices Involved

shiftens of

[redacted] WFO personnel

[redacted] BA

[redacted] HO

? JK

[redacted] SF

b6
b7C

[redacted] BS

? UNC

[redacted] NY

[redacted] LA

[redacted]

to be determined

288-HQ-1242560

from: ctac
to: ctac
2/14/98

288-HQ-1212560-209

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/03/1998

To: Criminal Investigative **Attn:** NIPC/CIU
Chicago **Attn:** 288 Supervisor
San Francisco **Attn:** 288 Supervisor

From: [redacted]
Squad 4
Contact: SA [redacted]

b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted] :tjm

Case ID #: 288-HQ-1242560 -211 (Pending)
[redacted] -108

Title: SOLAR SUNRISE;
CITA/NIPC

Synopsis: Information is being forwarded to receiving offices regarding captioned matter.

Details: On 4/3/98, SA [redacted] Kansas City Division (KCD), telephonically contacted [redacted] MOREnet Network and Security Services (MNSS), 1805 E. Walnut Street, Columbia, Missouri 65201, telephone number [redacted] fax number (573) 884-6673, regarding a fax received from [redacted] on 3/6/98. The fax described an intrusion into a computer at the Central Methodist College, cmc2.cmc.edu, which is a downstream connection from MNSS.

b6
b7C

[redacted] advised that someone named [redacted] sent an E-mail message to MNSS with a password file attached. The password file was later verified as an old password file from cmc2.cmc.edu. [redacted] claimed he received the password file from an "east coast" hacker who claimed to be involved with the compromises of the Pentagon servers via the Internet. The hacker sent the password file to [redacted] as proof of his hacking ability.

b6
b7C

[redacted] later learned that [redacted] was a [redacted] for the publication AntiOnline, web address: www.antionline.com. [redacted] advised [redacted] chatted with [redacted] using Internet Relay Chat (IRC), and that [redacted] was the one who sent [redacted] the password file.

b6
b7C

11887

b6
b7C

b6
b7C

A copy of the aforementioned fax is attached.

This information is being forwarded to receiving offices for whatever action deemed appropriate.

♦♦

MOREnet
The Missouri Research and Education Network ✦ 1805 East Walnut Street ✦ Columbia, Missouri 65201
(573) 884-7200 ✦ FAX - (573) 884-6673 ✦ World Wide Web - http://www.more.net ✦ E-mail - info@more.net

March 6, 1998

TO: SA [redacted]

COMPANY: Federal Bureau of Investigation, Kansas City Field Office

ADDRESS:

PHONE:

FAX: [redacted]

FROM: [redacted]

Missouri Research and Education Network
1805 E. Walnut St.
Columbia, MO 65201

PHONE: [redacted]

FAX: (573) 884-6673

b6
b7C

MESSAGE: Following is a summary of the current incident we are working on. Feel free to contact me with anything you need further on this. I look forward to meeting and working with you!

Best regards;

[redacted]

MOREnet Security Services
Incident Summary: MN#12696

Tuesday, 3 Mar 98 approx 2241 CST MOREnet received a page from [redacted] at ISCA regarding a security incident with one of our downstream connections. [redacted] the MOREnet Security Coordinator responded to [redacted]'s call and learned that he was in possession of a password file, reportedly from a computer designated cmc2.cmc.edu

The computer designated is located at Central Methodist College, connected via MOREnet to the Internet. The Internic Whois table lists MOREnet as the technical contact, which precipitated [redacted] call to us.

[redacted] reported that he received the file from an 'east coast' hacker who was claiming to be involved with the recent compromises of the Pentagon and other servers via the Internet. He was sent the file as verification of the hacker's abilities.

After exchanging PGP keys, [redacted] forwarded the file to us on 4 Mar 98 via electronic mail from an account [redacted] We forwarded the file to [redacted] the system administrator at Central Methodist College who confirmed file was indeed the password file from the cmc2.cmc.edu computer as it appeared in late 1996 or early 1997. Related note; we had an incident in November of 1996 wherein the same server was compromised and the password file was suspected to have been cracked at that time.

b6
b7C

On 5 Mar 98 at approx 1445 CST, [redacted] at Central Methodist reported that he observed a userID logged into the cmc2.cmc.edu system at IP Address [redacted] that was attempting to install COPS, a commonly used UNIX system cracking tool [redacted] terminated the user session, and within a few minutes noticed that another userID logged into the system and attempted the same installation. [redacted] noted and reported to us that the sessions were connecting via telnet from a system identified as dyn4.kaskad.ru at IP Address [redacted] terminated the second session, and as of 1630 CST had not had further login attempts from outside of the College's network.

At approx 1500 CST, MOREnet reported the incident to CERT. CERT's suggestion was to send email to the network provider for kaskom.ru with the incident information. CERT requested to be cc'd on the email note. [redacted] from MOREnet sent this note at approx 1700 CST. MOREnet recommended to Central Methodist that the server be taken off line, have the operating system installed from known media and patched to the current levels before bringing the system back online. MOREnet further blocked the IP address [redacted] at the site router, preventing further network traffic to and from the system.

Nothing Further.
[redacted] MOREnet Network and Security Services
5 Mar 98 1730CST

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 3/5/98

[redacted] HARVARD UNIVERSITY, Oceanography Group, 29 Oxford Street, Cambridge, Massachusetts, date of birth [redacted] was advised of the identity of the investigating agent and the purpose if the interview. [redacted] provided the following information:

b6
b7C

[redacted] was aware that the Oceanography's Computer System had been compromised. [redacted] advised that his identification had been used extensively by the hacker. [redacted] gave permission to copy all files in his directories for analysis by the FEDERAL BUREAU OF INVESTIGATION.

Investigation on 3/3/98 at CAMBRIDGE, MASSACHUSETTS

File # 288-HQ-1242560 Date dictated 3/4/98

by SA [redacted] aa b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 3/5/98

[redacted] HARVARD UNIVERSITY, Oceanography Group, 29 Oxford Street, Cambridge, Massachusetts, date of birth [redacted] telephone [redacted] was advised of the identity of the investigating agent and the purpose of the interview. [redacted] provided the following information: b6 b7C

[redacted] was aware that the Oceanography's Computer System had been compromised. [redacted] advised that his identification had been used by the hacker. [redacted] gave permission to copy all files in his directories for analysis by the FEDERAL BUREAU OF INVESTIGATION (FBI). [redacted] advised that he had created a directory named HACK and had placed files left in his directories by the hacker into that directory.

Investigation on 3/3/98 at CAMBRIDGE, MASSACHUSETTS

File # 288-HQ-1242560 Date dictated 3/4/98

by SA [redacted] jad aa b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

11887 439

b6
b7C
b7E

1001 MAI 00012

PP RHCNFB FBIJK FBIBA FBISF FBIBS FBIJL FBIHO FBILV
FBINY FBICE FBIDE FBICG FBIKC FBIHN

DE FBINF #0002 0450009

ZNY SSSSS

P 1400Z FEB 98

FM FBI WASHINGTON FIELD [redacted] (288-HQ-1242560)

TO DIRECTOR FBI/PRIORITY/

FBI JACKSONVILLE/PRIORITY/

FBI BALTIMORE/PRIORITY/

FBI SAN FRANCISCO/PRIORITY/

FBI BOSTON/PRIORITY/

FBI DALLAS/PRIORITY/

FBI HOUSTON/PRIORITY/

FBI LAS VEGAS/PRIORITY/

FBI NEW YORK/PRIORITY/

FBI CHARLOTTE/PRIORITY/

FBI DETROIT/PRIORITY/

FBI CHICAGO/PRIORITY/

FBI KANSAS CITY/PRIORITY/

FBI HONOLULU/PRIORITY/

288-HQ-1242560-227

BT

ORIGINAL FILED IN

PAGE TWO DE FBIWF 0002 ~~SECRET~~

~~SECRET~~

CITE: //3920//

PASS: AUC [redacted] FBIHQ; ROOM 11687.

b6
b7C

SUBJECT: UNSUB(S); [redacted] US NAVY - VICTIM; CITA -

INTRUSION. OO:WFO.

UNSUB(S); MULTIPLE INTRUSIONS INTO DOD FACILITIES; CITA -

INTRUSION. OO:HQ

REF NUMEROUS TELCALLS BETWEEN WFO AND FBIHQ, CITAC

BEGINNING 2/6/98 AND TELCALL BETWEEN SSA [redacted] WFO, AND SA [redacted] b6
b7C

SE, ON 2/13/98.

[redacted]

Referral/Consult

Referral/Consult

[redacted]

[redacted] IT IS ALSO ANTICIPATED THAT WFO CASE AGENT WILL BE REQUIRED TO TRAVEL TO JACKSONVILLE DIVISION TO REVIEW THE EVIDENCE SECURED BY THE VICTIM SITE AND CONDUCT OTHER INVESTIGATIVE STEPS POTENTIALLY NECESSARY. Referral/Consult

[redacted]

[redacted] Referral/Consult

BOTH THESE INVESTIGATIONS ARE OF SIGNIFICANT CONCERN GIVEN POTENTIAL MILITARY OPERATIONS IN THE MIDDLE EAST. FBIHQ AND WFO WILL KEEP AFFECTED DIVISIONS FULLY APPRISED OF SIGNIFICANT DEVELOPMENTS AS APPROPRIATE.

ANY QUESTIONS REGARDING THESE MATTERS SHOULD BE DIRECTED TO AUC [redacted] FBIHQ, CITAC, [redacted] QUESTIONS REGARDING WFO'S INVOLVEMENT SHOULD BE DIRECTED TO SSA [redacted] b6 b7C

[redacted]

BT

#0002

NNNN

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

11887
4315

0001 MRI 00023

OO P12 FBIPH FBINK

DE FBIWF #0001 0490022

ZNY SSSSS

O 180021Z FEB 98

FM FBI WASHINGTON FIELD (288-HQ-1242560)

TO DIRECTOR FBI/IMMEDIATE/

FBI PHILADELPHIA/IMMEDIATE/

FBI NEWARK/IMMEDIATE/

BT

~~S E C R E T~~

CITE: //3920//

PASS: AUC [redacted] FBIHQ, RM 11887; SSA [redacted] b6 b7C

FBIHQ CART; SA [redacted] NEWARK.

SUBJECT: OPERATION SUNRISE; CITA - INTRUSION.

REF TELCALLS BETWEEN WFO, FBIHQ CART, FBIHQ CITAC ON 2/17/98.

BEGINNING IN JANUARY 1998 AND CONTINUING THROUGH INSTANT DATE, UNKNOWN SUBJECTS HAVE BEEN SUCCESSFULLY INTRUDING UPON NUMEROUS UNITED STATES NAVY AND AIR FORCE COMPUTER NETWORKS

235

CC-4315

LOCATED THROUGHOUT THE UNITED STATES. THESE ATTACKS ARE BEING LAUNCHED FROM VARIOUS IP ADDRESSES, LOCATED AROUND THE WORLD. DUE TO THE SOPHISTICATION OF THE ATTACKS AND THE POTENTIAL ACCESS TO SENSITIVE MILITARY INFORMATION, THE DEPARTMENT OF DEFENSE IS TAKING AN AGGRESSIVE POSTURE T RESOLVE THESE MATTERS AS SOON AS POSSIBLE. FBIHQ, CITAC, HAS BEEN COORDINATING THE INITIAL PHASES OF THE INVESTIGATION. HOWEVER, WFO IS BEING ASKED TO COORDINATE A SIGNIFICANT AMOUNT OF THE INVESTIGATION BOTH WITHIN THE WASHINGTON, DC AREA AND IN OTHER LOCATIONS THROUGHOUT THE U.S. THIS COORDINATION INCLUDES LIAISON WITH U.S. AIR FORCE, OFFICE OF SPECIAL INVESTIGATIONS (OSI); THE DEFENSE INFORMATION SYSTEMS AGENCY (DISA); DEPARTMENT OF JUSTICE COMPUTER CRIME UNIT; AS WELL AS THE SERVICE UPON VARIOUS TELECOMMUNICATIONS ENTITIES OF NUMEROUS COURT ORDERS. THIS INVESTIGATION IS OF SIGNIFICANT CONCERN GIVEN POTENTIAL MILITARY OPERATION IN THE MIDDLE EAST.

Referral/Consult

Referral/Consult

[redacted]

SSA [redacted] CART, FBIHQ HAS ADVISED THAT NO CART EXAMINERS ARE AVAILABLE IN EITHER PHILADELPHIA OR BALTIMORE DIVISIONS AND REQUESTED THAT THIS LEAD BE ASSIGNED TO SA [redacted] NEWARK DIVISION. b6 b7C

ANY QUESTIONS REGARDING THIS MATTER SHOULD BE DIRECTED TO AUC [redacted] FBIHQ, CITAC, [redacted] QUESTIONS REGARDING WFO'S INVOLVEMENT SHOULD BE DIRECTED TO SSA [redacted] b6 b7C

LEAD:

AT NEWARK, NEW JERSEY:

CART IS REQUESTED TO MAKE A MIRROR IMAGE COPY OF THE HOME COMPUTER BELONGING TO [redacted] PROVIDED CONSENSUAL SEARCH AUTHORITY FOR CART TO CONDUCT THIS EXAMINATION. b6 b7C

[redacted] ADVISED THAT HIS COMPUTER CONTAINS WINDOWS 95, 2.5

GIGABYTE HARDDRIVE, ONE (1) 5 1/4" AND ONE (1) 3 1/2" FLOPPY DRIVES, ON CD ROM DRIVE, AND APPROXIMATELY FIFTY (50) 3 1/2" FLOPPIES. THIS LEAD IS REQUESTED TO BE COVERED AS EXPEDITIOUSLY AS POSSIBLE.

BT

#0001

NNNN

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-25-2012 BY [redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/13/1998

To: San Francisco **Attn:** SA [redacted]

From: NSD/CID
NIPC/CIU/Rm 11887
Contact: SSA [redacted]

b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]:heg

Case ID #: 288-HQ-1242560-237 (Pending)
[redacted] ending)
ending)

Title: Solar Sunrise;
CITA Matters;
00:HQ

Synopsis: To provide copies of FD-302's and 1-A's relevant to SF investigation of [redacted]

Enclosures: The following FD-302's are enclosed: [redacted] dated 2/19/98, [redacted] dated 2/19/98, [redacted] dated 2/17-19/19, [redacted] dated 2/17/98, [redacted] dated 2/13/98. The following 1-A's are enclosed: From [redacted] dated 2/18/98, from [redacted] dated 2/19/98, from [redacted] date 2/19/98, from [redacted] dated 2/23/98, from [redacted] dated 2/17/98.

b6
b7C

Details: The NIPC has been receiving responses to leads set out under 288-HQ-1242560. The responses received may relate to or impact SF investigations of [redacted] Copies of all material received by NIPC will be forwarded to SF for review.

♦♦

UPLOADED BY SDH 4/13/98